ELSEVIER

Discrete Mathematics 260 (2003) 275–283

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

Classification of Hadamard matrices of order 44 with automorphisms of order 7 ☆

Svetlana Topalova[1]

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, P.O. Box 323, 5000 Veliko V. Tarnovo, Bulgaria

Received 16 May 2000; received in revised form 1 May 2001; accepted 14 May 2001

Abstract

The Hadamard matrices of order 44 possessing automorphisms of order 7 are classified. The number of their equivalence classes is 384. The order of their full automorphism group is calculated. These Hadamard matrices yield 1683 nonisomorphic 3-(44,22,10) designs, 57932 nonisomorphic 2-(43,21,10) designs, and two inequivalent extremal binary self-dual doubly even codes of length 88 (one of them being new). © 2002 Elsevier Science B.V. All rights reserved.

Keywords: Hadamard matrix; Design; Self-dual code; Automorphism

1. Introduction

Refer to 1,2,5, or 28 for the basic concepts and notations concerning Hadamard matrices and combinatorial designs, and to 1 or 25 for different methods for construction of self-dual codes from designs.

A *Hadamard matrix of order n* is an $n \times n$ (± 1)-matrix satisfying $HH^t = nI$ (its rows are pairwise orthogonal). Two Hadamard matrices are *equivalent* if one can be transformed into the other by a series of row or column permutations and negations. An *automorphism* of a Hadamard matrix is an equivalence with itself. Each Hadamard matrix can be normalized, i.e. replaced by an equivalent Hadamard matrix

☆ Electronic Annexes available. See http://www.elsevier.com/locate/disc

[1] This work was partially supported by the Bulgarian National Science Fund under Contract No. I-803/1998. Some of the results were partially announced at the Second International Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, 1998, and at the Seventh International Workshop on Algebraic and Combin. Coding Theory, Bansko, Bulgaria, 2000.

E-mail address: svetlana@moi.math.b2s.bg (S. Topalova).

PII: S0012-365X(02)00400-4

whose first row and column entries are 1-s. Deleting the first row and column of a normalized Hadamard matrix of order $4m$, and replacing -1-s by 0-s, you obtain a symmetric 2-$(4m-1, 2m-1, m-1)$ design which is called a Hadamard 2-design. Let V be the set of points of this design, and $\mathscr{B}$ its set of blocks. A Hadamard 3-$(4m, 2m, m-1)$ design can be constructed with a point set $V \cup \{\infty\}$ and blocks $\{V \setminus B : B \in \mathscr{B}\} \cup \{B \cup \{\infty\} : B \in \mathscr{B}\}$.

Hadamard matrices have extremely interesting combinatorial properties, and various applications 6. There has been a continuous interest in their studies. Hadamard matrices of orders up to 28 have been fully classified (for order 28 see 15 and an alternative classification in 23, for 24 12,14, and for orders up to 24 a summary in 1). Only partial classifications are available for orders 32, 36 and 40 24,27, because the computational complexity of the classification problem rises exponentially.

Classification methods similar to those used in the present work have been used for instance in 13,26,27, but Hadamard matrices of order 44 have not been classified up to now. The present partial classification was only possible after a careful consideration of the symmetry of the tactical configurations arising from 2-(43,21,10) designs with automorphisms of order 7.

Two Hadamard 2-(43,21,10) designs have been constructed 19 with automorphisms of order 43 9. One of them can also be obtained by Paley's theorem 22. This paper offers a classification of all the inequivalent Hadamard matrices of order 44 possessing automorphisms of order 7 (our study shows that their number is 384), and their corresponding 3-(44,22,10) and 2-(43,21,10) designs (their numbers are 1683 and 57932, respectively).

The first known extremal binary doubly even self-dual code of length 88 18 can be found using one of the 2-designs with an automorphism of order 43 (the one that was first constructed by Paley's theorem 22, and has a full automorphism group of order $903 = 3.7.43$). Recently, one more code of these parameters was constructed 10, and thus two inequivalent extremal doubly-even self-dual [88,44,16] codes were known up to this work.[2]

The methods used in this paper for constructing self-dual codes from symmetric designs are well described in 3,29. In the present work all the binary doubly even self-dual codes of length 88 arising this way from the 2-(43,22,11) designs were tested. There are two extremal codes among them, the one being new.

In 7, the possible weight enumerators of self-dual codes of length 86 are determined and an extremal self-dual [86,43,16] code is constructed. It is the only one known by now. In the present work plenty of self-dual codes of length 86 were constructed from the 2-designs found, but none of them is extremal.

The approach used in this study implies the following: All the 2-(43,21,10) designs with automorphisms of order 7 were found first. Their number appeared to be 886. A Hadamard matrix was constructed from each design. These matrices were then normalized in all the possible ways, and thus the nonisomorphic 3- and 2-designs they lead to were found. The number of the equivalence classes of Hadamard matrices with

[2] While the paper was refereed one more self-dual [88,44,16] code was constructed 21 which cannot be obtained from the designs in this work.

automorphisms of order 7 was established in three different ways. Binary self-dual codes of lengths 86 and 88 were constructed from the 2-(43,21,10) designs. As far as designs extendable to one and the same Hadamard matrix yield the same code, codes were constructed from only one design of each Hadamard matrix set of nonisomorphic designs.

2. On the possible automorphisms of 2-(43,21,10) designs

Proposition 2.1. *All the possible prime divisors of the order of the group of automorphisms of a* 2-(43,21,10) *design are* 2, 3, 5, 7 *and* 43.

Proof. If a 2-(v,k,λ) design possesses an automorphism of a prime order p, then $p \leqslant k$ or $p|v$. (Otherwise there should exist fixed points and blocks, all the fixed points should be in fixed blocks, and all the fixed blocks should only contain fixed points, thus forming a 2-(v,k,λ), i.e. all the points and blocks will be fixed.) Thus $p = 2,3,5,7,11,13,17,19,43$ are the only possible prime orders of automorphisms of this design. Consider $p = 11,13,17,19$. Suppose there exists an automorphism of order p fixing $f > 1$ points. In this case, fixed blocks may contain either k or $k-p$ fixed points. Let us denote by h_1 and h_2 the number of fixed blocks containing, respectively, k and $k-p$ fixed points. Then, the following system holds.

$$\binom{21}{2} h_1 + \binom{21-p}{2} h_2 = \binom{f}{2} \lambda,$$

$$h_2 \leqslant \frac{43-f}{p},$$

$$h_1 + h_2 = f \geqslant 1,$$

$$h_1 + h_2 \leqslant 43 - p.$$

This system has no solution in integers. The cases $f = 0,1$ are only possible if $p|v$ or $v = 1 \pmod p$, respectively. Thus, a 2-(43,21,10) design cannot possess automorphisms of prime orders $11,13,17,19$. □

Proposition 2.2. *An automorphism of order* 7 *of a* 2-(43,21,10) *design fixes one point and one block.*

Proof. Suppose a 2-(43,21,10) design possess an automorphism of order 7 fixing $f > 1$ points and blocks. An automorphism of a symmetric design can fix at most half of the points 8,16,4. That is why $f = 8$ or 15. A fixed block might contain the points of m nontrivial point orbits, and thus $v - 7m$ fixed points ($m = 1,2,3$). Yet, if a fixed block has no fixed points, its common points with any other fixed block will not be 10 (but they should be because the design is symmetric). That is why fixed blocks can have either 7 or 14 fixed points. Let us denote by h_7 and h_{14} the fixed blocks containing 7, and 14 fixed points, respectively.

Suppose $f=15$. In this case, there are 4 nontrivial point orbits. Two fixed blocks cannot contain the points of the same two nontrivial point orbits, thus $h_7 \leqslant \binom{4}{2}=6$. But $h_{14} \leqslant 1$ (otherwise two blocks will contain more than 10 common points), and thus $f \leqslant 7$—contradiction.

Suppose $f=8$. There are five nontrivial point orbits, and thus at least two blocks containing the points of one and the same nontrivial point orbit. These blocks must meet in exactly 3 fixed points—impossible. □

3. Construction of 2-(43,21,10) designs with automorphisms of order 7

Designs with the biggest possible automorphism groups possess a lot of symmetry, and can usually be constructed more easily. Seven is the greatest possible prime order of an automorphism of a 2-(43,21,10) design which has not been considered yet.

Let D be a 2-(43,21,10) design with an automorphism α of order 7 with one fixed point and one fixed block. Without loss of generality, we can assume that α acts on the points (blocks) as follows:

$\alpha=(1,2,3,4,5,6,7)(8,9,10,11,12,13,14)\cdots(36,37,38,39,40,41,42)(43)$.

The automorphism α determines a circulant structure of the incidence matrix A of the design D, and A should be of the form

$$A=\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & u^t \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & u^t \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & u^t \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & z^t \\ a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & z^t \\ a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & z^t \\ u & u & u & z & z & z & 0 \end{pmatrix},$$

where $a_{i,j}$, $i,j=1,2,\ldots,6$ are circulant matrices of order 7, $u=(1,1,1,1,1,1,1)$, $z=(0,0,0,0,0,0,0)$.

Let $m_{i,j}$, $i,j=1,2,\ldots,6$ be equal to the number of 1's in a row of $a_{i,j}$. The following six equations hold for the matrix $M=(m_{i,j})_{6\times 6}$. (The first four ones are obtained by calculating in two ways the number of points and point pairs in the ith circulant row of A, and the last two by calculating the number of point pairs for which the first point is from the i_1st, and the second from the i_2nd circulant row.)

$$\sum_{j=1}^{6} m_{i,j}=20, \quad \sum_{j=1}^{6} m_{i,j}^2=74, \quad i=1,2,3,$$

$$\sum_{j=1}^{6} m_{i,j}=21, \quad \sum_{j=1}^{6} m_{i,j}^2=81, \quad i=4,5,6,$$

$$\sum_{j=1}^{6} m_{i_1,j} m_{i_2,j} = 63, \quad 1 \leqslant i_1 < i_2 \leqslant 3,$$

$$\sum_{j=1}^{6} m_{i_1,j} m_{i_2,j} = 70, \quad 1 \leqslant i_1 < i_2, \ \ i_2 > 3.$$

There are two nonisomorphic matrices M_1 and M_2 for which the upper equations hold.

M_1

5	2	3	4	4	2
3	5	2	2	4	4
2	3	5	4	2	4
4	4	2	5	2	4
2	4	4	4	5	2
4	2	4	2	4	5

M_2

4	4	2	5	3	2
2	4	4	2	5	3
4	2	4	3	2	5
5	2	3	3	5	3
3	5	2	3	3	5
2	3	5	5	3	3

Let us consider the matrix A'.

$$A' = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & u^t \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & u^t \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & u^t \\ \bar{a}_{4,1} & \bar{a}_{4,2} & \bar{a}_{4,3} & \bar{a}_{4,4} & \bar{a}_{4,5} & \bar{a}_{4,6} & z^t \\ \bar{a}_{5,1} & \bar{a}_{5,2} & \bar{a}_{5,3} & \bar{a}_{5,4} & \bar{a}_{5,5} & \bar{a}_{5,6} & z^t \\ \bar{a}_{6,1} & \bar{a}_{6,2} & \bar{a}_{6,3} & \bar{a}_{6,4} & \bar{a}_{6,5} & \bar{a}_{6,6} & z^t \\ z & z & z & u & u & u & 0 \end{pmatrix}, \tag{1}$$

where $\bar{a}_{i,j}$ can be obtained from $a_{i,j}$ by replacing 0 by 1 and 1 by 0. It is easy to check that A' is an incidence matrix of a 2-(43,21,10) design with automorphisms of order 7 too, and that if A corresponds to M_1, A' corresponds to M_2 and vice versa. The two designs can be extended to equivalent Hadamard matrices. That is why to construct all the 2-(43,21,10) designs possessing automorphisms of order 7 it is enough to extend only one of the matrices M_1 and M_2.

The replacement of the elements of M_1 with circulants of order 7 is the most difficult part of the present research. To make the programs finish in reasonable time, the symmetry of this matrix was used. All the possible ways to extend each row (column) were found first. Then while matching them together, both row and column properties were taken into consideration.

The extension of M_1 leads to the construction of 443 nonisomorphic 2-(43,21,10) designs. Then 443 designs corresponding to M_2 were obtained from them. The automorphism groups of all the 886 nonisomorphic designs were calculated. Two of the designs are isomorphic to the designs found in 9. One of them has a full automorphism group of order 903, the other 301. There are 81 designs with a full group of automorphisms of order 21—five self-dual ones and 38 pairs of dual designs. The order of the automorphism groups of the remaining 804 designs is 7.

4. Equivalence classes and automorphism groups of Hadamard matrices of order 44 with automorphisms of order 7

Let H and $\bar{H}$ be two Hadamard matrices of order n, such that the elements of the first one equal the elements of the second multiplied by -1. We shall denote by H^* the matrix

$$H^* = \begin{pmatrix} H & \bar{H} \\ \bar{H} & H \end{pmatrix}.$$

To determine the equivalence classes of Hadamard matrices, the following statement can be used.

Two Hadamard matrices H_1 and H_2 are equivalent iff the matrices H_1^* and H_2^* are equivalent.

This statement was proved in graph notations in 20. As far as automorphism means equivalence with itself, it follows that

The order of the full automorphism group of a Hadamard matrix H is the same as the order of the full automorphism group of H^*.

In slightly different notations the upper was also formulated and used by Ito 11.

The equivalence classes of the constructed Hadamard matrices were determined by three independent methods. The same result was obtained, and this is some guarantee for its correctness.

The first approach used to establish (in)equivalence of two Hadamard matrices H_1 and H_2 is by checking for (in)equivalence of the matrices H_1^* and H_2^* . It is very convenient to start with this method as it will remove the equivalent matrices, and a smaller number of Hadamard matrices will be checked by the other two methods (which are not so fast) just to confirm their nonequivalency.

By the second method all the 2-(43,21,10) designs arising from the Hadamard matrices are generated and the sets of 2-designs corresponding to these matrices are compared.

The third method is similar to the second one, but the 3-designs are concerned. This way 57932 nonisomorphic 2-(43,21,10) and 1683 nonisomorphic 3-(44,22,10) designs were constructed. All the 2-designs obtained which do not possess automorphisms of order 7, do not possess any automorphisms at all.

Equivalence tests were made much faster by using suitable invariants, i.e. for each row (column) i of H^* the vector $(m_0, m_1, \ldots, m_{10})$ was calculated where m_s is the number of triples of rows (columns) j, k, l, different from i and such that there are s columns containing 1s in each of the rows i, j, k, l. If we sort these vectors lexicographically, we obtain an invariant of the Hadamard matrix. All the 384 equivalence classes are fully distinguished by these invariants.

The order of the full automorphism group was also calculated. Algorithms for determining the order of the automorphism group of Hadamard matrices are known (see for instance 17), but in the present work the order of the full automorphism group of H^* was found instead. This was done using the algorithm (and respectively the author's program) for calculating the order of the automorphism group of a 2-design.

Table 1
Order of the full automorphism group of the Hadamard matrices

$\lvert\mathrm{Aut}(H)\rvert$	Number of matrices	2-designs	3-designs	Comments
$79464 = 2.44.43.21$	1	2	1	22
$602 = 2.43.7$	1	10	2	9
$84 = 4.21$	40	48	2	
$28 = 4.7$	284	140	4	
$14 = 2.7$	58	280	8	

The number of Hadamard matrices with certain automorphisms is presented in Table 1, where the number of 2- and 3-designs they yield is also given. The last column refers to other works in which these designs were constructed and studied.

There is only one matrix with a transitive group of automorphisms. It is the one from the Paley series. The order of its full automorphism group is 79464. The matrix corresponding to the other design found in 9 has a group of order 602. There are 40 Hadamard matrices of order 44 (two self-dual ones and 19 pairs of dual matrices) whose order of the full automorphism group is 84.

5. Construction of self-dual codes

Let A_{21} be the incidence matrix of a 2-(43,21,10) design, A_{22} the incidence matrix of the corresponding 2-(43,22,11) design, and

$$A_{22}^{+} = \begin{pmatrix} A_{22} & U^t \\ U & 0 \end{pmatrix},$$

where U is the all-one vector of dimension 43.

Then $(A_{21}\ I_{43})$ is a generator matrix of a self-dual code of length 86. Yet the self-dual codes thus constructed are of minimum weight at most 14.

A generator matrix of a doubly even self-dual code of length 88 can be obtained as $(A_{22}^{+}\ I_{44})$. Two inequivalent extremal [88,44,16] codes can be obtained this way. The first one is generated by the Paley matrix 22 and is equivalent to one of the codes already known. The other one can be obtained as indicated above from a design with the following base blocks:

$B_1 = 2\ 3\ 9\ 10\ 12\ 16\ 17\ 18\ 20\ 21\ 23\ 25\ 27\ 30\ 31\ 32\ 34\ 35\ 37\ 38\ 39\ 43$
$B_8 = 2\ 3\ 4\ 5\ 7\ 8\ 11\ 16\ 20\ 21\ 24\ 27\ 28\ 31\ 32\ 33\ 36\ 37\ 39\ 41\ 42\ 43$
$B_{15} = 2\ 3\ 4\ 5\ 6\ 8\ 10\ 12\ 15\ 18\ 19\ 22\ 24\ 27\ 28\ 29\ 30\ 31\ 34\ 35\ 37\ 42$
$B_{22} = 2\ 3\ 6\ 8\ 13\ 14\ 15\ 17\ 19\ 20\ 21\ 22\ 23\ 25\ 27\ 28\ 29\ 33\ 37\ 38\ 39\ 41$
$B_{29} = 2\ 3\ 5\ 8\ 11\ 12\ 13\ 14\ 15\ 17\ 22\ 23\ 24\ 25\ 26\ 30\ 32\ 35\ 36\ 39\ 42\ 43$
$B_{36} = 2\ 4\ 6\ 9\ 10\ 11\ 13\ 14\ 19\ 20\ 21\ 24\ 25\ 30\ 33\ 34\ 35\ 36\ 37\ 39\ 40\ 42$

To show that this code is not equivalent to any of the two extremal binary self-dual codes of length 88 known by now 7, the following invariants were calculated for each

of the three codes: There are 32164 vectors of minimum weight 16 in the code. We consider them as rows of a (0,1) matrix and calculate for each column of the matrix a vector of its scalar products with the other 87 columns. The entries of these vectors and the vectors themselves are sorted lexicographically, and thus an invariant of the code is obtained. The three codes are fully distinguished by these invariants.

It is worth pointing out here that two of the three known extremal binary self-dual doubly-even codes of length 88 are obtained from Hadamard matrices, and that the Hadamard matrix leading to the new extremal code has an automorphism group of order 14 only.

References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge Tracts in Mathematics, Vol. 103, Cambridge University Press, Cambridge, 1992.
[2] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1993.
[3] V.K. Bhargava, J.M. Stein, (v,k,λ) configurations and self-dual codes, Inform. and Control 28 (1975) 352–355.
[4] A.R. Camina, A survey of the automorphism groups of block designs, J. Combin. Designs 2(2) (1994) 79–100.
[5] R. Craigen, Hadamard matrices and designs, The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 370–377.
[6] R. Craigen, W. Wallis, Hadamard matrices: 1893–1993, Congr. Numer. 97 (1993) 99–129.
[7] St. Dougherty, T.A. Gulliver, M. Harada, Extremal binary self-dual codes, IEEE Trans. Inform. Theory 43(6) (1997) 2036–2047.
[8] W. Feit, Automorphisms of symmetric balanced incomplete block designs, Math. Z. 118 (1970) 40–49.
[9] M. Hall, Jr., A survey of difference sets, Proc. Amer. Math. Soc. 7 (1956) 975–986.
[10] M. Harada, H. Kimura, On extremal self-dual codes, Math. J. Okayama Univ. 37 (1995) 1–14.
[11] N. Ito, On Hadamard groups, J. Algebra 168 (1994) 981–987.
[12] N. Ito, J.S. Leon, J.Q. Longyear, Classification of 3-(24,12,5) designs and 24-dimensional Hadamard matrices, J. Combin. Theory Ser. A 31 (1981) 66–93.
[13] H. Kimura, Hadamard matrices of order 28 with automorphism groups of order 2, J. Combin. Theory Ser. A 43 (1986) 98–102.
[14] H. Kimura, New Hadamard matrix of order 24, Graphs Combin. 5 (1989) 235–242.
[15] H. Kimura, Classification of Hadamard matrices of order 28, Discrete Math. 133 (1994) 171–180.
[16] E.S. Lander, Symmetric designs: an algebraic approach, London Mathematical Society, Lecture Note Series 74, Cambridge University Press, Cambridge, 1983.
[17] J. Leon, An algorithm for computing the automorphism group of a Hadamard matrix, J. Combin. Theory Ser. A 27 (1979) 289–306.
[18] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error—Correcting Codes, Elsevier, Amsterdam, 1977.
[19] R. Mathon, A. Rosa, $2-(v,k,\lambda)$ designs of small order, The CRC Handbook of Combinatorial Designs, CRC Press, New York, 1996, pp. 3–41.
[20] B. McKay, Hadamard equivalence via graph isomorphism, Discrete Math. 27 (1979) 213–214.
[21] A. Otmani, A new construction of self-dual codes, Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bansko, Bulgaria, June 2000, pp. 255–260.
[22] R.E.A.C. Paley, On orthogonal matrices, J. Math. Phys. MIT 12 (1933) 311–320.
[23] E. Spence, Classification of Hadamard matrices of orders 24 and 28, Discrete Math. 140 (1995) 185–243.
[24] E. Spence, Regular two-graphs on 36 vertices, Linear Algebra Appl. 226–228 (1995) 459–497.
[25] E. Spence, V.D. Tonchev, Extremal self-dual codes from symmetric designs, Discrete Math. 110 (1992) 265–268.

[26] V.D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 7, J. Combin. Theory Ser. A 40 (1985) 62–81.
[27] V.D. Tonchev, Hadamard matrices of order 36 with automorphisms of order 17, Nagoya Math. J. 104 (1986) 163–174.
[28] V.D. Tonchev, Combinatorial Configurations, Longman Scientific and Technical, New York, 1988.
[29] V.D. Tonchev, Symmetric designs without ovals and extremal self-dual codes, Ann. Discrete Math. 37 (1988) 451–458.